Памятка участникам соревнований
по компьютерной безопасности VrnCTF

CTF (Capture The Flag) соревнования проводятся в двух форматах: Task-Based и Attack-Defense. Task-Based CTF фокусируется на решении отдельных задач и сбору флагов. Флаг – строка, подходящая под определенный формат, в случае с VrnCTF это будет строка вида vrnctf{some_text}. Для написания текста во флагах используется leet – язык, в котором буквы английского алфавита заменяются на цифры, например, фраза some_text может выглядеть как s0m3_t3xt.

В Attack-Defense формате, команды участников должны найти и проэксплуатировать уязвимости серверов соперников, одновременно с этим устраняя собственные уязвимости.

Задачи в Task-Based формате охватывают широкий спектр тем, связанных с информационной безопасностью, и могут быть как простыми, так и чрезвычайно сложными.

Стоит заметить, что для решения многих задач нужна операционная система на базе Linux. Подойдет развернутая на виртуальной машине. Чаще всего используют Kali Linux, так как на ней предустановлены многие полезные утилиты.

При этом задачи делятся на категории, самыми распространенными из которых являются:

Web – задачи, связанные с веб-безопасностью, такие как поиск уязвимостей XSS или SQL-инъекций, эксплуатация уязвимостей и захват флагов из веб-приложений. Поскольку наши соревнования ориентированы на новичков, никакие специализированные инструменты вам не понадобятся. Советуем почитать в интернете что такое SQLi, LFI, RCE. В изучении этих уязвимостей вам поможет HackTricks.

PWN – задачи, нацеленные на эксплуатацию уязвимостей в операционных системах и приложениях, часто с использованием техник реверс-инжиниринга и анализа двоичного кода.

Crypto – задачи, требующие криптографических знаний для шифрования, дешифрования, взлома хэшей и анализа криптографических протоколов. Минимум, который вам понадобится, – умение определить шифр и найти способ его дешифровать. В этом вам может сильно помочь онлайн сервис CyberChef, а также утилита RsaCtfTool для Linux.

Forensics – задачи, фокусирующиеся на анализе цифровых артефактов, таких как образы дисков, сетевой трафик и журналы, для извлечения информации и улик. На наших соревнованиях вам будет достаточно разобраться в работе платформы Splunk.

OSINT – задачи, в которых необходимо использовать навыки сбора и анализа информации из открытых источников. Самая нетребовательная к инструментарию категория. В большинстве случаев вам понадобится только поисковик. Небольшая рекомендация: поиск по картинкам лучше осуществлять в Яндексе.

Stego – задачи, связанные со скрытием информации в тексте и файлах, таких как изображения или аудио. Стеганография – метод сокрытия информации в другой информации. Для решения наших задач этой категории уже понадобится запустить Linux, нам будут нужны его инструменты. Прочитайте про работу таких утилит, как Steghide, Stegsolwe, Binwalk, Strings, File, что из себя представляют сигнатурные байты файлов, а также о структуре файлов.

Revers – задачи, требующие навыков реверс-инжиниринга для анализа и модификации программного обеспечения. Помимо обширных знаний о структуре программ и файлов вам понадобятся такие инструменты, как IDA,

HEX redactor, x32/64 dbg для тех, кто работает на Windows и Radare с Ghydra для Linux.

PPC (программирование) – задачи на программирование (чаще сетевое), или автоматизацию обработки большого количества данных. Тут вам понадобится знание языков программирования и алгоритмов.

Misc – категория, охватывающая широкий спектр задач, не подпадающих под другие категории, от стеганографии до криптографии.

Для решения задач вам понадобится внимательность и смекалка. Подсказки могут быть в названии и тексте задачи. Подсказкой может оказаться что угодно.

Перечисленного должно хватить, чтобы принять участие в нашем соревновании, и взять старт для погружения в мир информационной безопасности.